GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

November 30, 2001

The Honorable Jerry Lewis
Chairman, Subcommittee on Defense
Committee on Appropriations
House of Representatives

Subject: <u>Joint Warfighting: Attacking Time-Critical Targets</u>

Dear Mr. Chairman:

This letter responds to your request that we review the Department of Defense's (DOD) efforts to enhance its ability to attack time-critical targets.[1] While DOD has developed and fielded considerable capability to detect, assess, and attack most fixed enemy targets, experiences in the Persian Gulf and more recently in Kosovo revealed that DOD has limited ability to rapidly identify and strike time-critical targets, such as mobile Scud[2] and surface-to-air missile sites. Such targets proved to be elusive when our adversaries were able to move critical assets to safety in a shorter time frame than it takes us to implement the sensor-to-shooter process. In fact, the time needed to effectively attack mobile targets is much shorter than DOD's established 30 to 72 hour targeting cycle for attacking most fixed targets.

DOD studies have pointed to a variety of reasons for why it takes too long to be in a position to strike time-critical targets. Chiefly, the systems involved in the sensor-to-shooter process do not operate effectively together. There are over 100 command, control, communications, intelligence, surveillance, and reconnaissance systems that are needed to identify and strike targets. But these are separately owned and operated by each of the military services as well as other DOD and intelligence agencies. These separate systems have limited ability to interoperate, both technically (such as incompatible data formats) and operationally. As a result, they cannot easily and quickly exchange data; communication systems must be patched together to make this happen. Compounding this problem is the fact that each service has its own command, control, and communications structure that may present barriers to interoperability. In fact, in a battle situation, the Joint Forces Commander is faced with integrating, in an ad hoc manner, more than 400 different mission and software applications.

---

[1] These include targets that are of high value, require immediate response, or have a limited window of vulnerability such as mobile theater missiles, surface-to-air missile launchers, and cruise missile batteries.

[2] Scud missiles are mobile, short-range surface-to-surface missiles.

20011211 160

DOD has undertaken numerous efforts to address these fundamental problems. Primarily, DOD has developed guidance to help the military services achieve system interoperability[3] as well as oversight controls, directives, and policies to ensure that this guidance was being followed and that interoperability is being achieved. DOD has also worked to develop joint capabilities through exercises and advance concept technology demonstrations. The demonstrations focus on assessing emerging technologies, such as those that would put targeting information into the hands of commanders faster as well as new manned and unmanned sensors and weapons platforms. Additionally, the individual services have undertaken a variety of efforts to improve their own capability to attack time-critical targets. For example, the Air Force is developing a new family of systems designed to attack time-critical targets much more quickly. The Navy has an effort to network its sensors, command centers, and long-range weapons. And the Army is working to improve the flow of battlefield information.

While these efforts are helping DOD to make improvements in the sensor-to-shooter process, considerably more needs to be done to significantly reduce the time it takes to strike time-critical targets. First, DOD needs to overcome cultural impediments to joint warfighting. Each of the military services still plans, acquires, and operates systems to effectively meet its own operational concepts, but not necessarily the requirements of joint operations. To facilitate the services' different capabilities and concepts of operation requires segmenting the battlefield with each military component responsible for a specified area of the battlefield. And there is little incentive to design common, integrated[4] systems. Naturally, this continues to result in disparate systems. The Joint Chiefs of Staff reported that there are over 100 different operational architecture efforts. DOD's Director for Interoperability also estimates that there are $36 billion worth of systems the services plan to buy that cannot operate effectively together.

Second, some of DOD's current oversight and control mechanisms are simply not working. For example, DOD's Joint Interoperability Test Command (JITC) is the primary certifier for ensuring that the military services' command, control, communications, and intelligence systems are interoperable and are able to exchange information effectively during a joint mission. But DOD organizations have not always complied with the interoperability testing and certification process. Furthermore, according to a Defense Science Board study, the Joint Interoperability Test Command does not have the facilities needed to test the interactions between the services' weapon systems and information systems. The Joint Chiefs of Staff has also recognized that its Joint Requirements Oversight Council (JROC)—which is responsible for approving the services' operational requirements for high-valued systems—has not been focused on evaluating systems from a joint warfighting perspective.

---

[3] Interoperability is essentially the ability of independent systems to provide and accept information from other systems.

[4] Integrated systems extend beyond interoperability to form a network of interdependent systems. Such integrated systems are expected to provide increased capabilities over disparate independent systems that are capable of exchanging information.

Third, DOD still lacks a joint service concept of operations to defeat time-critical targets and, as a result, each military service plans and acquires systems to meet requirements under its own concept of operations. A joint operational concept would provide the necessary foundation for developing joint requirements for common integrated systems. Once a joint operational concept is developed, a joint operational architecture needs to be constructed to focus on how the services will work together to carry out joint warfighting missions and help ensure that their operations are in synchronization. Ultimately, this should lead to an enterprise architecture that would include joint operational concepts and operational architectures, along with comprehensive systems architectures. A comprehensive systems architecture would provide the underlying blueprint for more detailed design and implementation decisions about component systems. With a complete architecture, DOD would be able to ensure that duplicative as well as disparate systems are not allowed to go forward.

During our review, we discussed these and other problems with senior officials in the military services and in DOD and found general agreement as to the causes of the problems and additional steps needed. These steps are captured in a number of recent DOD plans and initiatives. Importantly,

- The 2001 Quadrennial Defense Review reinforces previous guidance by stating that DOD must integrate combat forces and they must be highly networked with joint command and control. The Review calls for developing a standing joint task force that will develop an operational concept to address the critical operational challenge—to continuously locate and track and attack time-critical targets. The headquarters for these new forces would provide uniform standard operating procedures, tactics, techniques, and technical system requirements. The standing joint task force would undertake experimental exercises as new technologies become available.

- In a July 2001 report, *Network Centric Warfare*, DOD proposed establishing an Office of Transformation to ensure adequate focus on improving joint network-centric warfighting capabilities and to help overcome impediments to progress such as cultural, organizational, and other barriers. It stated that network-centric warfare and operations should be the cornerstone of DOD's strategic plan for transformation of the forces. The 2001 Quadrennial Defense Review reported plans to appoint a Director for Force Transformation to foster innovation and experimentation, who will report to the Secretary and Deputy Secretary of Defense.

- The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence recently issued a strategic plan for integrating intelligence, surveillance, and reconnaissance systems.

- The Joint Chiefs of Staff is developing joint operational concepts and architectures that are needed to achieve joint integrated warfighting capabilities. The U.S. Joint Forces Command is also developing joint operational concepts, including time-critical targeting, as well as conducting joint experiments and testing of its new warfighting concepts in collaboration with the services.

- The Joint Chiefs of Staff is strengthening reviews conducted by its Joint Requirements Oversight Council to ensure that individual systems establish interoperability as a key performance parameter (requirement). The Joint Requirements Oversight Council also plans to change its approach to its review of major systems' operational requirements by ensuring that they have a more "joint" focus that addresses the warfighters' needs rather than a "service" focus.

These and other new efforts are further described in enclosure I.

It is too early to determine whether these steps will enable DOD to overcome the challenges associated with achieving more common, integrated systems necessary for effectively attacking time-critical targets. As such, we will continue to monitor these initiatives. In particular, we plan to monitor whether and how well DOD is overcoming impediments such as cultural barriers. Undoubtedly, this will be the most critical challenge for DOD. Past efforts to focus on system development from a DOD-wide perspective versus a service-perspective have failed because the services were unwilling to forego their unique requirements in favor of requirements that would benefit the department as a whole. At the same time, DOD did not have a sustained commitment from its top leaders or did not successfully implement management policies and funding controls needed to overcome service resistance.

We also plan to monitor whether and how well DOD develops, implements, and enforces a joint concept of operations and a joint operational architecture. Our previous reviews have shown that while the absence of a complete architecture does not guarantee the failure of system modernization efforts, it does greatly increase the risk that agencies will spend more time and money than necessary to ensure that systems are compatible and in line with mission needs. Again, however, developing a joint concept of operations and a joint operational architecture, and ultimately an enterprise architecture, will be extremely challenging because it will require DOD to obtain consensus from the services and others on high-level issues such as creating a joint command and control structure—something that has not yet been achieved on such a large scale.

Lastly, we plan to monitor whether DOD is putting in the right tools to guide its efforts to success. These include a central clearinghouse to review and coordinate the implementation of the many different service and DOD initiatives to reduce the risk of overlap and duplication and increase opportunities for knowledge sharing. These also include specific guidance on where DOD specifically wants to go in terms of systems interoperability so that oversight and control entities have a solid foundation for deciding whether individual efforts will complement each other and link to DOD's overall goals.

Agency Comments

DOD provided oral comments on a draft of this report. DOD noted that our report makes several pertinent observations and that it would consider our comments when addressing solutions. It further stated that the recent Defense Planning Guidance has placed emphasis on attack of time-critical targets. DOD also provided technical corrections that we incorporated where appropriate.

Scope and Methodology

During our review we analyzed an extensive array of DOD policy, planning, and guidance documents, official publications, statements, reports and other assessments, and open literature addressing attacking time-critical targets, interoperability, and joint warfighting capabilities to develop a better understanding of the key issues affecting progress. We also met with a broad spectrum of key defense officials in various offices and commands to discuss the problems facing the military in attacking time-critical targets, the need for integrating the capabilities necessary for detecting, tracking, communicating, deciding, and attacking time-critical targets; and the need for developing a joint concept of operations which would provide the framework for determining the joint warfighting requirements that would be critical in developing new or modified systems needed to attack time-critical targets. DOD offices visited included the Office of the Secretary of Defense (Acquisition, Technology, and Logistics; Command, Control, Communications and Intelligence; and Operational Test and Evaluation); the Joint Staff; the U.S. Joint Forces Command; the Air Force's Air Combat Command and Aerospace Command and Control, Intelligence, Surveillance, and Reconnaissance Center; the Navy Warfare Development Command; service representatives; and others.

We conducted our review from February 2000 to October 2001 in accordance with generally accepted government auditing standards.

Unless you publicly announce its contents earlier, we plan no further distribution of this report until 5 days from its issue date. At that time, we will send copies of this report to the Secretary of Defense, the Secretary of the Air Force, the Secretary of the Army, the Secretary of the Navy, the Commandant of the Marine Corps, and the Chairman, Joint Chiefs of Staff. We will make copies available to others on request and through the GAO home page at http://www.gao.gov.

We plan to keep you informed on the results of our monitoring efforts that relate to DOD's efforts to improve interoperability and shorten the time needed to strike time-critical targets. In the interim, if you have questions about the initiatives described in this letter or the challenges DOD now faces, please call me at (202) 512-4841. Other major contributors to this work include William Gillies and Mary Quinlan.

Sincerely yours,

James F. Wiggins
Director
Acquisition and Sourcing Management

Enclosure

Description of Recent Initiatives to Address Interoperability Problems

Quadrennial Defense Review

Summary: This review was intended to develop a new strategy for the defense of the United States. Decisions taken on strategy, forces, capabilities, and risks resulted from months of deliberation and consultation among senior Department of Defense (DOD) leadership.

The review calls for developing new joint forces that come under joint command and control and that are highly networked. The forces would be lighter, more lethal and maneuverable, survivable, and more readily deployed and employed in an integrated fashion.

To enable a common relevant operational picture of the battlespace, the review calls for enhancing communications networks and systems to provide shared situational awareness and integration of joint fires, maneuver, and intelligence.

The review calls for establishing a standing joint task force headquarters, which would provide uniform, standard operating procedures, tactics, techniques, and technical system requirements, with the ability to move expertise among commands. The headquarters is to have a standardized operational architecture.

The review states that DOD will examine the option of establishing a standing joint task force to address the critical operational challenge of locating, tracking, and attacking mobile targets at any range with precision.

The review also calls for undertaking experimental exercises, as new technologies become available.

Status: Report issued September 2001.

Report on Network-Centric Warfare

Summary: This report to the Congress was directed by section 934 of the National Defense Authorization Act for Fiscal Year 2001 (P. L. 106-398).

Network-centric warfare is described as a set of warfighting concepts and associated military capabilities that allow warfighters to take advantage of all available information and bring all available assets to bear in a rapid and flexible manner.

Network-centric warfare is not a fully developed and deployable warfighting capability. In fact, applications of network-centric warfare theory have been limited, but early experimentation has shown justification for its impact on future combat forces.

DOD's strategy for implementing network-centric warfare is to (1) set priorities in developing and implementing network-centric concepts and capabilities, such as the capability to self-synchronize its operations, and achieve secure and seamless connectivity, (2) measure success, and (3) overcome obstacles that are cultural, organizational, technical and administrative. To ensure adequate focus in implementing this strategy, an Office of Transformation, reporting to the Secretary of Defense, will be established.

The report acknowledges that each service is actively acquiring service-centric time-critical targeting capabilities without an integrating effort to address a joint architecture.

Status: Report issued July 2001.

Intelligence, Surveillance, and Reconnaissance Integrated Capstone Strategic Plan

Summary: The Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, issued this plan to provide a structure and methodology for guiding intelligence, surveillance, and reconnaissance toward an integrated capability to maintain information superiority. DOD envisions a system that brings together a joint and combined force of national, theater, and tactical sensors, commanders and shooters to strike targets rapidly at extended ranges. DOD also envisions a new operational concept to attack time-critical targets that integrates command and control authorities; command and control, intelligence, surveillance, and reconnaissance systems; and, shooters.

Status: Plan issued November 2000.

Joint Chiefs of Staff/ U.S. Joint Forces Command

Summary: Revised Joint Chiefs of Staff (JCS) Instruction designated interoperability as a (mandatory) key performance parameter for systems that exchange information. Interoperability requirements must be addressed in the operational requirements document approved by the Joint Requirements Oversight Council and evaluated by the U.S. Joint Forces Command based on a warfighter's perspective. Interoperability key performance parameters will be tested and certified by the Joint Interoperability Test Command.

The JROC plans to change its approach to its review of major systems' operational requirements by ensuring that they have a more "joint" focus that addresses the warfighter's need rather than a service focus.

JCS is planning to develop, using its Joint Warfighting Capabilities Assessments, joint operational concepts for its critical warfighting functions, including precision engagement and dominant maneuver. These operational concepts will guide future sensor to shooter system acquisitions. They will also serve as a foundation for joint operational architectures that will provide the framework for developing a system-of-systems solution to time-critical targeting.

The U.S. Joint Forces Command is responsible for developing new operational concepts, including attacking time-critical targets, and executing joint experimentation as it develops new joint warfighting concepts.

Status: The JCS's instruction "Interoperability and Supportability of National Security Systems, and Information Technology Systems" (CJCSI 6212.01B) was issued May 2000.

Global Information Grid (GIG)

Summary: The Global Information Grid provides a very broad high-level concept to integrate information capabilities and is expected to meet the needs of the individual services as they develop solutions to address the limitations in attacking time-critical targets. The advancement of the global information grid would benefit from incorporating joint operational concepts as it forms architectures needed in developing joint warfighting capabilities.

Status: Ongoing.

The Family of Interoperable Pictures (FIOP)

Summary   The Family of Interoperable Pictures (FIOP) is a methodology for addressing the lack of a coherent view of the battlefield. The Office of the Under Secretary of Defense/Acquisition, Technology, and Logistics, Interoperability is the lead proponent for the FIOP and the JROC has directed implementation of a strategy, to be led by the Air Force, to develop a joint concept of operation needed to provide an all-source picture of the battlefield. This initiative requires that a joint concept of operations be developed before developing requirements.

Status   Ongoing.

Air Force Efforts

Summary   The Air Force is developing a new family of systems to attack time-critical targets that are expected to reduce attack times. For example, the time-critical targeting cell initiative will provide the air component commander's air operations center an ability to detect and direct forces to attack targets quickly. The theater battle management core system is expected to merge several legacy systems such as its air tasking order system, which controls employment of fixed wing aircraft in the battle area with new capabilities, to reduce the timelines to attack time-critical targets.

Status   Ongoing.

Navy Efforts

Summary   The Navy is developing a new series of systems for its time-critical strike future naval capability program, such as the real time execution decision support (REDS) initiative.

           The Navy is also working on a network-centric warfare concept that will network Navy sensors, command centers, and its long-range weapons to attack a broader range of targets (including those in the deep battle area) more effectively. This concept includes a vast array of procurement and research and development weapon systems, ships, aircraft, and command and control, communications, intelligence and reconnaissance programs.

           The Navy is considering the need for new command and control ships to provide the Navy with the capability to control deployed joint forces while stationed off shore.

Status   Ongoing.

Army Efforts

Summary   The Army is continuing to fund its Battlefield Digitization initiative, which is designed to improve the flow of battlefield information within the Army's fighting organizational structure.

           The Army is also developing a transformation strategy, which is designed to ensure that the Army could respond to a broad range of operations. The strategy centers on developing a combat force that is expected to be lighter, but just as powerful and survivable as today's heavy force. This new force will be planned around Future Combat systems. These systems will provide the capability to attack critical targets much deeper in the battle area before they become a direct threat.

Status   Ongoing.

(120028)